



# **Exploring the Interactions Between Network Data Analysis and Security Information/Event Management**

**Timothy J. Shimeall  
CERT® Network Situational Awareness  
(NetSA) Group  
January 2011**



Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE <b>JAN 2011</b>		2. REPORT TYPE		3. DATES COVERED <b>00-00-2011 to 00-00-2011</b>	
4. TITLE AND SUBTITLE <b>Exploring the Interactions Between Network Data Analysis and Security Information/Event Management</b>				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) <b>Carnegie Mellon University,Software Engineering Institute,Pittsburgh,PA,15213</b>				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT <b>Approved for public release; distribution unlimited</b>					
13. SUPPLEMENTARY NOTES <b>FloCon 2011, in Salt Lake City, Utah, on January 10-13, 2011.</b>					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT <b>Same as Report (SAR)</b>	18. NUMBER OF PAGES <b>11</b>	19a. NAME OF RESPONSIBLE PERSON
a. REPORT <b>unclassified</b>	b. ABSTRACT <b>unclassified</b>	c. THIS PAGE <b>unclassified</b>			

---

© 2011 Carnegie Mellon University

## NO WARRANTY

THIS MATERIAL OF CARNEGIE MELLON UNIVERSITY AND ITS SOFTWARE ENGINEERING INSTITUTE IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This presentation may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu).

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

CERT® is a registered mark owned by Carnegie Mellon University.

# Overview

---

Network Data

Security Information/Events

The Problem

Events, Revisited

Analysis leading to Events

The Problem, Revisited

Summary

# Network Data

---

larger network, more security data

Data: Packets, Flows, DNS resolutions, host log entries, firewall log entries, etc.

Data (in general) -> Low security information density

Analysis (in part) -> Use goal/context to focus on higher-density data subsets, convert to aggregated form



# Security Information/Events

---

Commonly: “Event: Something that happens”

SIEM: Event:

- Something describable via the schema
- Instance of security-sensitive activity observed at a device
- Aggregations of security-sensitive activity
- Chains of security-sensitive activity

Information: Context for analyzing or processing events

# The Problem

---

If “generation of data instance” = “event”, too many events

- For collection and processing
- For human analysts

Candidate solutions:

- Sampling
- Reduce data on arrival
- Restrict scope
- Restrict classes of data

# Events, Revisited

---

Definition: “Security sensitive event -- instance of activity that, in context, is associated with a threat to the network or with its defensive strategy.”

Security sensitivity depends on context

Effective security depends on strategy

Edge devices (router, firewall, proxy, etc.) can not have that context (or time to process it)



# Analysis as Event Mediator

---

Event mediator: Automated actors receiving instances of network activity and applying context and strategy information to filter for security-sensitive events.

Application:

- Process-mapping approach, isolating critical “tipping points” sensitive for security
- Rule-based approach, identifying specific events with high security sensitivity
- Learning approach, using historical data to build indicators of security sensitivity

All three approaches are based on analysis.

# Moving Closer to Reality

---

Mediators provide more achievable information distribution

- Core-outward: context information, strategy rules
- Edge-inward: filtering (and re-filtering) event stream to isolate security sensitivity.

Mediators simplify handling

- By automation: fewer intervening cases
- By humans: lower event rates

# The Problem, Revisited

---

## How often to publish context

- Rule updates
- Repeated training

## How to incorporate strategy

- Deception
- Frustration
- Resistance
- Isolation/Recovery

# Summary

---

Initial definition of security sensitive event

Decomposition of problem

Strategies for further development

Experience and experimentation needed